UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/801,614	03/08/2001	Gerald Francis McBrearty	AUS9-2000-0935-US1	5324

7590   07/25/2008

International Business Machines Corporation
Intellectual Property Law Department
Internal Zip 4054
11400 Burnet Road
Austin, TX 78758

EXAMINER
DENNISON, JERRY B

ART UNIT	PAPER NUMBER
2143	

MAIL DATE	DELIVERY MODE
07/25/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Application Number: 09/810,614
Filing Date: March 19, 2001
Appellant(s): HSIAO, CHAI-I

_____
J. B. Kraft
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed 27 May 2008 appealing from the Office

action mailed 26 December 2007.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The following are the related appeals, interferences, and judicial proceedings known to the examiner which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal:

Cross-referenced Application, SN. 09/810,612, G. F. McBrearty et al. filed on March 08, 2001, concurrently with the present Application is on Appeal before the Board of Appeals.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

2002/0069363	Winburn	6-2002
7,150,045	Koelle et al.	12-2006
6,647,400	Moran	11-2003

Powell, Keith A, "The Waite Group's Windows 98 How-To", Sams Publishing, January 1999, 3 pages

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1, 5, 7, 10, 14, 17, 31 and 33 are rejected under 35 U.S.C. 102(e) as being anticipated by Winburn (U.S. 2002/0069363).

1.   Regarding claims 1, 5, 7, 10, 14, 17, 31 and 33, Winburn disclosed, in a data

processing operation having stored data in a plurality of data files, a system (Winburn,

Fig. 1, system 10) for protecting said data files from unauthorized users comprising:

        means for storing for each of said plurality of data files, a backup file inaccessible

to user requests (Winburn, [0026], Winburn disclosed an authentic backup file, with its

identity and location camouflaged to remove any direct relation between any of the

attributes of the authorized protected data file and the corresponding authentic backup

file);

        means for receiving user requests for access to data files (Winburn, [0025],

Winburn disclosed user accesses to authorized protected data files);

        means for determining, without accessing any of said backup files (Winburn,

[0008], Winburn disclosed "an identifier is stored and used to test the content of the

current protected data file to determine if the current protected data file is the same as

the authorized protected data file or has been changed without authorization", which

clearly indicates that the identifier is used for determining, not the backup file), whether

said requests are unauthorized intrusions into said requested data files (Winburn,

[0030], Winburn disclosed, in response to a sensed event, checking the protected data

file to see if it has been changed without authorization, thereby determining if a user

access/request was unauthorized);

        means responsive to an initial determination that a request is unauthorized for

destroying the requested data files (Winburn, [0026], Winburn disclosed reconstructing

the last authorized copy of the protected file into the protected file, which requires

destroying the previous tampered file, i.e. it no longer exists; Fig. 7, 69, Winburn

disclosed "delete compromised current protected data file); and

means for reloading a backup file for each destroyed file (Winburn, [0026], Fig. 6,

61, Winburn disclosed recovering the authentic backup and restoring the authorized

protected data file; Fig. 7, Winburn disclosed "Write restored authorized protected data

file" by clearly using the backup file).

Claims 5 and 7 include a system with limitations that are substantially similar to

claim 1, including use in business transactions, including "e-commerce" which inherent

to include web sites (see Guheen U.S. 7,165,041). Claims 10, 14, and 17 include a

method with limitations that are substantially similar to claim 1. Claims 21, 25 and 27

include a computer program (Winburn, [0032]) with limitations that are substantially

similar to claim 1. Claims 31 and 33 include a computer-readable medium with

limitations that are substantially similar to claim 1. Figure 8 of Winburn shows many

examples of computer readable media. Therefore, claims 5, 7, 10, 14, 17, 31 and 33

are rejected under the same rationale.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

Claims 4, 13, 20, 32, 34, and 35 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Winburn (U.S. 2002/0069363) in view of Moran (U.S.6,647,400) and

Koelle et al. (U.S. 7,150,045).

2.   Regarding claims 4, 13, 20, 32 and 35, Winburn disclosed the limitations,

substantially as claimed, as described in claims 1, 10, 17, 31 and 33. Winburn also

disclosed detecting unauthorized access of data without authority into a data system

(Winburn [0002]), and checking the protected data file to see if it has been tampered in

response to a sensed event (Winburn, [0030]).

Therefore, while Winburn disclosed detecting unauthorized accesses based on

sensed events, Winburn did not provide explicit examples of sensed events that would

trigger the system to check for such unauthorized access/tampering of the files.

This would have motivated one of ordinary skill to search the prior art for well-

known triggers that identify unauthorized accesses into a system.

In analogous art, Moran disclosed different intrusion detection triggers including

password-guessing attacks (Moran, col. 24, lines 40-45), and Koelle disclosed detection

of unauthorized client behaviors including unauthorized copying of protected data

(Koelle, see Abstract).

Winburn suggests detecting unauthorized intrusions into the system. Moran and

Koelle provide explicit examples of well-known intrusion detection techniques.

Therefore it would have been obvious to one of ordinary skill in the art at the time the

invention was made to incorporate the techniques of Moran and Koelle into the system

of Winburn in order to provide a system that is more secure to attacks from

unauthorized users for the benefit of providing a more reliable system.

3.   Regarding claim 34, Winburn disclosed the limitations as described in claim 33.

Winburn also disclosed a use for the invention to be with "e-commerce transactions."

        Winburn did not explicitly state wherein the network is the World Wide Web and

said network sites are Web sites.

        However, maintaining security and protecting from intrusion into hosts of

websites on the World Wide Web was well known in the art at the time of the invention.

Therefore, since the teachings of Winburn disclosed techniques for protecting against

intrusion, then one of ordinary skill in the art would have been motivated to use the

teachings of Winburn to maintain security on websites on the World Wide Web. In

addition, Winburn disclosed a use for the teachings to be through "e-commerce". One

example of "e-commerce" that was well known before the invention was made is

Ebay.com, which is clearly an e-commerce website on the World Wide Web. As such, it

would have been obvious for one of ordinary skill in the art at the time the invention was

made to incorporate the teachings of Winburn into a website on the World Wide Web for

the purpose of increasing security on websites such as Ebay.com to prevent intruders

from making falsifying e-commerce transactions.

(10) Response to Argument

Applicant did not provide separate arguments with respect to the rejections of claims 1,
4, 5, 7, 10, 13, 14, 17, 20, 31-35. Applicant provides a single argument with respect to
a limitation recited in the independent claim 1. Therefore, it appears that claim 1 is
representative of the cited claims, and as such, claims 4, 5, 7, 10, 13, 14, 17, 20, 31-35
stand or fall together with representative claim 1. 37 C.F.R. § 41.37(c)(1)(vii)

Applicants present a single principal argument:

"Winburn fails to teach the element of determining, <u>without accessing any of said</u>
<u>backup files</u>, whether said user requests are unauthorized intrusions into said requested
data files" (Br. 13-14).

Applicant attempts to show that Winburn fails to teach this limitation by alleging,
"in order to create the identifiers from the content of his backup files, Winburn must
access such backup files" (Br. 14, ¶1-2).

Regarding Applicant's argument that Winburn fails to teach determining,
without accessing any of said backup files, Examiner respectfully disagrees.

Examiner notes that Applicant has <u>failed to provide any explicit showing</u> that the
teachings of Winburn ***"must"*** access his backup files. Applicant is <u>merely alleging</u> that
this "accessing of backup files" must occur since the identifiers are created based on
attributes of the backup files.

Explanation of the Winburn reference

Winburn disclosed that "an algorithm…as would be known to those skilled in the art is used to produce from at least one attribute of the authorized protected data file, an identifier of the authorized protected data file". Winburn further disclosed that this identifier is stored (Winburn, page 1-2, [0008]).

Later on in the reference, Winburn disclosed, "The monitoring process…uses the identifier stored in the recovery address group and a test identifier produced from the current protected data file to determine if the current protected data file used to produce the test identifier is the same as the authorized protected data file" Winburn further disclosed that the test identifier is created in response to for example a sensed event (Winburn, [0029]).

In summary, from this citing, Winburn disclosed creating identifiers based on attributes of files and storing them. Then, when a sensed event occurs, a test identifier is created and used to determine if the current protected data file has been changed by comparing it with the identifier that was previously stored.

Obtaining attributes from a file does not require accessing the file

In a conventional sense, well known in the art, obtaining attributes of a file **does not require** accessing the file itself. A well known example of this can be shown using general purpose computing, using any Windows operating system such as Windows 95 or Windows 98 (which were produced well before Applicant's invention). It was within

the knowledge of one of ordinary skill in the art at the time the invention was made to obtain file attributes, not by accessing the file itself, but by simply going to the directory that the file is located. Reading a directory of files provides many attributes of each file within that directory, such as file name, file type, file size, date created, date modified, and location of the file. All of these attributes are clearly provided within the directory without actually executing or accessing any of the files themselves.

To provide evidence of this fact, Examiner provides the reference by Powell, titled, "The Waite Group's Windows 98 How-To" which was published in January 1999. Page 3 of this reference provides a display of a directory in Figure 6.21, titled, "Checking out the non-critical archives on your computer." This figure shows the "Archives" directory with multiple files within the directory. None of these files are being accessed. The display provides attributes for each file such as Name, Type, Size, Date, and Location. None of these files are being accessed to obtain these attributes. They are just simply provided within the directory.

As shown by the Powell reference, obtaining attributes from a file does not require accessing the file itself. Therefore, Applicant's allegation that the teachings of Winburn must access the backup files is believed to be in error.

For argument sake, let us assume that "creating the identifiers" does require accessing the backup files. Examiner notes that Winburn still meets the requirements of the independent claims.

The limitation recites, "determining, without accessing any of said backup files, whether said requests are unauthorized intrusions into said requested data files."

It is only the determination step that is performed without accessing the backup files.

As shown in Winburn, the identifiers are produced and stored in memory (Winburn, [0029]). Therefore, the identifiers are created and stored **before** any requests are made**.** As such, it is **before the determination step** that the identifiers are created (or for argument sake that the backup files are accessed).

The determination step itself only uses the identifier. The backup files are never accessed for the determination step. As such, Winburn disclosed determining, without accessing any of said backup files, whether said requests are unauthorized intrusions into said requested data files, exactly as the claims require.

In summary, Examiner has provided evidence that obtaining attributes from a file does not require accessing the file, and even if it did require accessing the file, Winburn still meets the claim limitations since creating the identifiers stored in memory occurs before any requests are made, and therefore before the determination can be made, since the determination requires the request to be made. As pointed out above,

Applicant has failed to provide any explicit showing that the teachings of Winburn

accesses the backup files. Therefore, in conclusion it believed that the teachings of

Winburn do not access the backup files in order to determine whether said user

requests are unauthorized intrusions into said requested data files, as claimed.

For at least these reasons, the rejections of claims 1, 5, 7, 10, 14, 17, 31, and 33

under 35 U.S.C. 102(e) and the rejections of claims 4, 13, 20, 32, 34, and 35 under 35

U.S.C. 103(a) is believed to be proper.

(11) Related Proceeding(s) Appendix

There has been no decision as yet in the Appeal before the Board in related

Cross-referenced Application, SN. 09/801,612, G. F. McBrearty et al. filed on March 08,

2001, concurrently with the present Application as mentioned above in section II.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/J. D./

J. Bret Dennison

Examiner, Art Unit 2143

/Nathan J. Flynn/

Supervisory Patent Examiner, Art Unit 2143

Conferees:

/Nathan J. Flynn/

Supervisory Patent Examiner, Art Unit 2143

/John Follansbee/

Supervisory Patent Examiner, Art Unit 2151